



Waymaker LLP
777 S. Figueroa Street, Suite 2850
Los Angeles, California 90017
T 424.652.7800

Author's Direct Dial No.
(424) 652-7814

Author's Email Address
bklein@waymakerlaw.com

By E-mail

August 30, 2021

AUSA Kimberly Ravener
AUSA Kyle Wirshba
United States Attorney's Office
Southern District of New York
1 Saint Andrews Plaza
New York, New York 10007

**Re: *United States v. Virgil Griffith,*
20 Cr. 15 (PKC)**

Dear Counsel:

We write in response to the government's August 21, 2021 expert disclosure and request for reciprocal disclosure from the defense.

Although we did not request expert notice pursuant to Federal Rule of Criminal 16(b)(1)(G) so no reciprocal disclosure is required, *see* Fed. R. Crim. P. 16(b)(1)(C)(i), in an effort to streamline these proceedings to preserve judicial and party resources, we inform you that, to the extent Mr. Griffith presents an affirmative defense case, he may call the following witnesses to offer expert testimony on the topics described below.

Andreas M. Antonopoulos

- As set forth in more detail in his *curriculum vitae*, which is attached, Mr. Antonopoulos is an expert in cryptocurrency, Bitcoin, Ethereum, and blockchain technology. He has worked almost exclusively in the blockchain industry since at least 2012. His education and professional qualifications to offer the below-described opinions are set forth in detail his *curriculum vitae*. Mr. Antonopoulos is more than qualified to offer his expected expert testimony.
- In forming his opinions, Mr. Antonopoulos has relied upon his education, knowledge, experience, and training in computer science and blockchain technology, as well as his



specific and extensive education, knowledge, experience, and training in the fields of computer science, blockchain technology, Ethereum, data communications, networks, and distributed systems. As part of the basis for his opinions, Mr. Antonopoulos may rely upon his own research and publications in this field as well as other similar cryptocurrency conferences he has attended at which Mr. Griffith and others presented the same or similar information to their audiences. Mr. Antonopoulos also has reviewed relevant portions of the government's discovery produced as of the date of this notice, as well as discovery produced by counsel for Mr. Griffith pursuant to his obligations under Rule 16(b)(1)(A).

- Based on the foregoing training and experience, as well as his review of discovery materials in this case, Mr. Antonopoulos is expected to offer the following background testimony:
 - Explain the background and characteristics of blockchain networks, including the culture and operation of open-sourced software, how decentralization works and secures these networks, and how tokens are created and used in blockchain networks.
 - Explain the terminology of cryptocurrency, which refers to certain blockchain token and is also called digital assets, that it is designed to work as a medium of exchange and/or a store of value, how types of cryptocurrencies (e.g., Bitcoin, Ether, *etc.*) differ, and the nature of the exchanges on which cryptocurrencies are transacted. (This will include a discussion of an Ether transaction involving 1 Ether, *i.e.*, what happens when a party “sends” 1 Ether to another party.)
 - Provide background information regarding Ethereum and the Ethereum Foundation, including but not limited to the Ethereum network’s creation, its unique contributions to blockchain development, the nature of its open-source software, including what applications use the network, the role that Ether tokens play on Ethereum, and the role Ether plays in the world of digital currency, as well as the function of the Ethereum Foundation and its goals.
 - Explain that an Internet Protocol address, commonly referred to as an “IP address” is a unique address that identifies a device on the internet or a local network. Internet Protocol is the set of rules governing the format of data sent via the internet or local network. Further:
 - In essence, IP addresses are the identifier that allows information to be sent between devices on a network: they contain location information and make devices accessible for communication. The internet needs a way to differentiate between different computers, routers, and websites. IP addresses provide a way of doing so and form an essential part of how the internet works.



AUSAs Ravener and Wirshba

August 30, 2021

Page 3 of 5

- Explain what a “VPN” is and how Internet users use VPNs to establish protected network connections when using public networks, including but not limited to the use and significance of encryption associated with VPNs when trying to determine the location or identity of a particular Internet user.
- As part of that background testimony, we expect that Mr. Antonopoulos will testify about the following terms of art, among others, that are relevant to the jury’s determination—and beyond the ken of the average person’s understanding—in this case:
 - Open-source software
 - Protocol specification
 - Ethereum Clients
 - Ethereum Network(s)
 - Ethereum Blockchain
 - Ether Currency
 - Ethereum Miners
 - Ethereum Nodes
- Based on the foregoing training and experience, as well as his review of discovery materials in this case, Mr. Antonopoulos is expected to offer the following expert opinions:
 - Nodes are not specific to Ethereum and perform a variety of purposes not limited to cryptocurrency or blockchain technology but more broadly relate to Internet and Internet access generally.
 - The information allegedly disclosed by Mr. Griffith at the Pyongyang cryptocurrency conference was neither unique to that conference nor prepared or tailored specifically to that conference and indeed consisted of publicly available information that could have been accessed by an individual with access to the Internet, including but not limited to similar presentations given by Mr. Griffith in other fora.
 - Nothing about the information presented by Mr. Griffith or others during the Pyongyang cryptocurrency conference was tailored to or otherwise unique to that particular event or locale. The information allegedly presented by Mr. Griffith was known ubiquitously in this industry and easily accessible to anyone with an Internet connection.

- VPNs are commonly used by nations like DPRK to avoid and evade sanctions, which otherwise would prohibit users in the DPRK or operating on behalf of the DPRK from accessing Internet services and networks.
- Individuals accessing the Internet from an ISP or IP address located in or traceable to the DPRK would not be able to access directly a U.S.-based ISP, including Verizon.net or Amazon Cloud Services.
- His observations based upon his review of the information provided by Oath, Inc. in response to a subpoena issued by counsel for Mr. Griffith.
- The Verizon records provide no basis to believe that the DPRK Email Account was accessed or otherwise acted upon within the Southern District of New York in response to Mr. Griffith's email to dprk.un@verizon.net. To the contrary, available information strongly supports the conclusion that it was not.
- The accuracy with which one could predict whether the DPRK Email Account was accessed from a location within the United States—let alone from within the Southern District of New York—is vanishingly small to non-existent and certainly well below a 50/50 chance.

Former OFAC Employee

The defense anticipates calling a former U.S. Department of Treasury Office in the Office of Foreign Asset Control ("OFAC") to testify about the following:

- The history, scope, and nature of the so-called Berman Amendment and the information and informational exemptions (collectively, the "Informational Exemption") to the IEEPA.
- OFAC's Office of Enforcement, its function and procedures in enforcing OFAC regulations through civil proceedings and the steps such a civil investigation would involve, as well as OFAC's coordination with the Department of Justice and U.S. Attorney's Offices.
- OFAC's enforcement of the NCSR regulations.
- How OFAC historically has applied the Informational Exemption to conduct that is pure speech, including but not limited to the significance of information being publicly available as opposed to being developed specifically for a particular presentation. As part of this opinion, we expect the expert will opine that an individual's protected speech would not be considered by OFAC to constitute a provision of services if the content of that speech and the information it disclosed was publicly available regardless of the sophistication of the audience.



AUSAs Ravener and Wirshba

August 30, 2021

Page 5 of 5

- The interplay between the IEEPA and OFAC sanctions as compared to the Commerce Department's export control regulations.
- Licensing determinations and OFAC enforcement actions related to activities that arguably qualify for protection under the Informational Exemption, as well as analogous situations involving the civil enforcement of other travel bans.

We have identified an expert who is prepared to offer opinions on the topic areas above based upon their prior experience with and employment by OFAC in enforcement. The expert has cleared conflicts. Given Mr. Griffith's incarceration and the due dates on the various filings in this case, we have been unable to meet with him to finalize the retention of the expert. We anticipate that we will be able to confirm the identity of the person and provide their *curriculum vitae* by the end of this week.

Mr. Griffith explicitly reserves the right to amend and/or supplement these disclosures based upon, among other things, additional discovery produced, counsel's ongoing review of the recent productions, trial preparation, disclosures about anticipated witness testimony, and ultimately the evidence (testimonial or opinion) offered in the government's direct case.

As always, we remain available to discuss this or any other aspect of the case.

Sincerely,

A handwritten signature in black ink, appearing to read "B. E. Klein".

Brian E. Klein
Keri Curtis Axel
Waymaker LLP

-and-

Sean S. Buckley
Kobre & Kim LLP

Attorneys for Virgil Griffith

Encl.

CURRICULUM VITAE
Andreas M. Antonopoulos
andreas@antonopoulos.com

ABSTRACT

Andreas M. Antonopoulos is a highly sought after world-class expert in Bitcoin, Ethereum and open blockchain technology. Andreas has been working exclusively in the Blockchain industry since 2012.

In 2014 O'Reilly Media published Andreas' first book, *Mastering Bitcoin*, a technical book for programmers. The book is widely viewed as the definitive guide on the subject and to date is the world's most cited book on Bitcoin.¹ In 2018, O'Reilly Media published "*Mastering Ethereum*", considered the canonical college-level textbook for Ethereum programming. Subsequently, Mr. Antonopoulos has published 4 additional books on the topics of bitcoin and open blockchains. Andreas' books, videos and articles have been translated into 31 languages cumulatively, both by commercial publishers and under open source licenses.

He has testified before regulators as an expert witness with respect to blockchain technology, once in 2014 before the Canadian Senate Banking and Commerce Committee and again in 2015 before the Economics References Committee of the Australian Senate.

In addition to his own projects within the industry, which demand the majority of his time, since 2014 he has served as a teaching fellow at the University of Nicosia, assisting with curriculum content and design, as well as co-teaching the *Introduction to Digital Currencies* course. Additionally, in 2014 he served as Chief Security Officer for blockchain.info, a well-known bitcoin wallet and block explorer.

Mr. Antonopoulos earned both his bachelors and masters degrees in Computer Science from University College London (UCL). At UCL, he studied networks and distributed systems while simultaneously working in IT. In fact, since 1990 Andreas has worked exclusively in the Information Technology sector, with an emphasis on networks, distributed systems, security, and training. He secured three patents for network technology inventions and has been published in peer reviewed journals as well as mainstream media sources.

Andreas has authored hundreds of syndicated articles on security, cloud computing, and data centers; and is a frequent keynote speaker at technology and security conferences worldwide. He has been interviewed by Bloomberg, CNN, CNBC, CBS, NBC, ABC, BBC, the Financial Times and many more media organizations for his industry expertise. He has been featured in numerous documentary films and is a permanent host on the Let's Talk Bitcoin podcast with more than 400 episodes recorded to date.

UNIVERSITY TEACHING AND RESEARCH

2014-to date	University of Nicosia - Teaching Fellow "M.Sc. Digital Currencies"
1995-1997	University College London - Research Fellow "Distributed Systems Lab"
1994-1995	University College London - Teaching Assistant "Internet and E-Commerce"
1992-1994	University College London - Computer Lab Assistant

EDUCATION

¹ According to a December 2nd, 2019 Google Scholar search

1994-1995	M.Sc. Data Communications Networks & Distributed Systems (DCNDS). University College London, London, UK. M.Sc. Project in cross-platform distributed data exchange framework as part of the EU (HANSA ESPRIT) funded project.
1991-1994	B.Sc. (Hons.) Computer Science. University College London, London, UK. B.Sc. Project in distributed collaborative computing, X-Windows screen-sharing protocol.

EXPERT WITNESS TESTIMONY

Canadian Senate Banking and Commerce Committee, presenting on Bitcoin and digital currencies, October 8, 2014.

Economics References Committee of the Australian Senate, presenting on Bitcoin and digital currencies, March 4, 2015

Kleiman v Wright, Expert Report and Depositions, 2020 (Trial scheduled November 2021)

PUBLISHED BOOKS

2014	<i>Mastering Bitcoin</i> , O'Reilly Media ² 2367 scholarly citations ³
2016	<i>The Internet of Money Volume 1</i> , Merkle Bloom 106 scholarly citations
2016	<i>Mastering Bitcoin 2nd Edition</i> , O'Reilly Media 227 scholarly citations
2017	<i>The Internet of Money Volume 2</i> , Merkle Bloom
2018	<i>Mastering Ethereum</i> , O'Reilly Media 330 scholarly citations
2019	<i>The Internet of Money Volume 3</i> , Merkle Bloom
2021 ⁴	<i>Mastering the Lightning Network</i> , O'Reilly Media 3 scholarly citations

KOREAN TRANSLATIONS OF PUBLISHED BOOKS

2015	<i>Mastering Bitcoin</i> , Korean Translation, Coinplug
2018	<i>Mastering Bitcoin 2nd Edition</i> , Coinplug <i>The Internet of Money, Volume 1</i>
2019	<i>Mastering Ethereum</i> , Korean Translation, J-Pub

² World's most cited book on bitcoin, according to Google Scholar

³ Citation counts by Google Scholar - updated August 2021

⁴ Due for publication Q4'2021

PUBLISHED ARTICLES

1998 - date More than 200 published articles and reports on Security, Data Centers, Cloud Computing and Cryptographic Currencies. (comprehensive listing available upon request)

INTERVIEWS

2012 - date More than 200 interviews on the topics of bitcoin and open blockchains including Bloomberg, CNN, CNBC, CBS, NBC, ABC, BBC, and Financial Times. (comprehensive listing available upon request)

PATENTS

System and Method for Securing Virtualized Networks USPTO 61/720,343

System and Method of Subnetting a Virtual Network Identifier, USPTO 14/210,069

System and Method for Dynamic Management of Network Device Data USPTO 9479P001

JOURNAL PUBLICATIONS

Peer-Reviewed Framework for Distributed Application Generation, SPEEDUP

Volume 11, Number 1, pp.15-17, Scientific Journal, (Jun. 1, 1997)

PROFESSIONAL HISTORY

2012 – to date **Founder, CEO** - aantonop Companies

Own and operate several companies focused on producing educational content about bitcoin and other open blockchains to people around the world. Manage a team of 11 people, producing videos, articles, interviews and books, public speaking, seminars, educational courses, and event management.

2014 - to date **Teaching Fellow** - University of Nicosia M.Sc Digital Currencies

Co-teach the open “MOOC” course for UNIC’s MSc programme in digital currencies., the world’s first university course in digital currencies. Curriculum development, teaching.

2014 Jan - Sep **Chief Security Officer** - Blockchain.info (bitcoin wallet and block explorer)

Served as the Chief Security Officer (CSO), coordinating strategy for security, secure software engineering practices, and security operations, email security anti-phishing operations.

2003 – 2011 **Founding Partner, CIO, Lead Security Research Analyst** - Nemertes Research

Developed and managed research projects, conducted strategic seminars and advised key clients as the lead analyst in Information Security, Data Center and Cloud Computing. CIO for the firm, managed a diverse cloud infrastructure supporting a distributed team. Responsible for HR and legal management. Founding partner and managing director.

2002-2003 **Director Security Practice** - ThruPoint Inc, NY

Directed a team of 70-80 network security, information security and penetration testing engineers, ensuring consistent delivery of consulting and professional services across a global delivery team. Lead for penetration testing (black box and red team) and vulnerability assessment of IT infrastructure systems including firewalls, file servers, email servers, PCI and HIPAA audits and bank trading systems. Supported sales efforts as team lead and promoted standardization of deliverables. Worked on accurately predicting and accounting for work effort, profit margin and project management in sales proposals.

2001 - 2002 **Security Practice Lead** - Greenwich Technology Partners, NY

Led the North East security practice, covering NY, NJ and CT, supporting sales operations (SME), delivering security advice and services and leading projects, including architecting a global secure financial transaction network for SWIFT. Penetration (black box) testing and vulnerability testing of production systems for financial services, healthcare and telecommunications companies.

2000 - 2001 **Founder** - Managed Business Network, London, UK
Consulting and integration services. This company was a successor to Phaia Limited.

1997-2000 **Managing Director** / Co-Founder - Phaia Limited, London, UK
IT services and system administration. Setup and administration of secure email, file server, collaboration and communication systems for financial services and other companies.

1997-2000 **Instructor - Security, Networking** - Learning Tree International, London, UK
Taught IT professionals 4-day intensive seminars on data communications, IT security, Internet protocols, operating system security, email security and network security. Highest rated instructor in Information Security for 2 years running.

1995-1997 **Research Fellow** - University College of London, Computer Science Department, London, UK
ESPRIT-funded interactive media project. External Lecturer. Lead Research Fellow, ``Distributed Application Generation'', EPSRC-funded project.

1995-1997 **Founder** - Athena Systems Design Limited, London, UK
IT consulting, systems administration, network installation, email servers, file servers.

1993-1995 **IT Manager** - Odey Asset Management, London, UK
Responsible for all IT at this legendary and pioneering british hedge fund. Systems administration, telecommunication, Internet security, email services, fax/telex servers, desktop support, trading systems (Reuters/Bloomberg), training.

1991-1993 **Freelance IT Consulting** - London, UK
IT support, systems administration, training

1990-1991 **Network Support Engineer, Trainer** - IBM Greece
Network installation, technical support, training.

Earlier work history available upon request



Amber Vitale

Managing Director
Forensic & Litigation Consulting

Three Times Square – New York, NY 10036

+1 646 453 1269

Amber.Vitale@fticonsulting.com

Education

B.S., Communications,
Ithaca College
J.D., Georgetown
University

Certifications

Admitted to the New York
Bar

Associations

Association of Certified
Sanctions Specialists
Association of Certified
Anti-Money Laundering
Specialists

Amber Vitale specializes in economic sanctions, anti-money laundering (AML) and anti-bribery/corruption compliance. Her expertise includes OFAC investigations; financial crimes-related regulation and compliance; and risk management and internal controls. She has 16 years of experience working on OFAC investigations and compliance matters involving numerous industries, including financial services, oil and gas, shipping, heavy equipment, agricultural and medical goods, among others. Amber has been a sanctions expert and liaison to investigators and prosecutors from federal, state and local agencies, such as the U.S. Department of Commerce, Department of Justice, and Manhattan District Attorney's Office.

Prior to joining FTI Consulting, Amber worked at OFAC for five years, including three as a Section Chief in Enforcement. Most recently, Amber was Head of Sanctions Advisory at Brown Brothers Harriman & Co. (BBH) where she was responsible for all sanctions investigations globally; OFAC disclosures and reports; developing enhanced processes and procedures; and providing sanctions compliance guidance and training.

In previous roles as a consultant to financial institutions, including as a Director in PwC's Financial Crimes Unit, Amber provided subject matter advice and led delivery teams focused on AML and OFAC-related projects. As an Associate at Schulte Roth & Zabel LLP, Amber provided legal counsel to banks, broker dealers, insurance companies, and money-service businesses, as well as investment advisors, fund managers and other global companies.

Relevant Experience:

- Assessed the global sanctions program of a financial services firm (one of the world's largest asset managers and custodians) and developed a Target Operating Model;
- Performed an enterprise-wide assessment of an investment firm's sanctions screening controls around transactions, documented screening processes and other controls, conducted gap analysis and recommended other risk-mitigating controls, and identified gaps in data sent for sanctions, PEP and negative news screening;
- Advised the New York branch of a non-U.S.-based global financial institution (world's largest multinational bank) regarding transition to FircoSoft, including drafting Business Requirements Document and Tuning and Testing Reports, and created test data and cases for User Acceptance and Functional Testing;
- Analyzed global custodian bank's (largest U.S. private bank) sanctions lists and FircoSoft algorithm and severity mode settings in preparation for NYSDFS Part 504 requirements; and
- Conducted OFAC investigations and drafted disclosures involving (1) securities-trade-related messaging services provided by a major U.S. company, (2) agricultural goods sold to Cuba by a U.S. company's Canadian subsidiary and related back-office services provided in the U.S., and (3) sales of nutritional products to Iran by a non-U.S. company that was acquired by a U.S. company.